

## Setup Steps for AIG Security

These are the general steps that must be followed in order to setup security properly for AIG.

**Note: Security groups can be edited at Start Page > System Administrator > Security > Groups**

**Note: Roles can be edited at Start Page > System Administrator > Roles Administration > User Access**

1. AIG District Coordinator – This person has full rights to the student AIG page and can edit records outside of any 30 day window.
  - a. Create AIG District Coordinator security group with default "View & Modify" access, and make sure this group can see at least one student screen (e.g., Demographics). The name of the group must be exactly as stated.
  - b. Create AIG District Coordinator role. The Description must be exactly as stated: AIG District Coordinator.

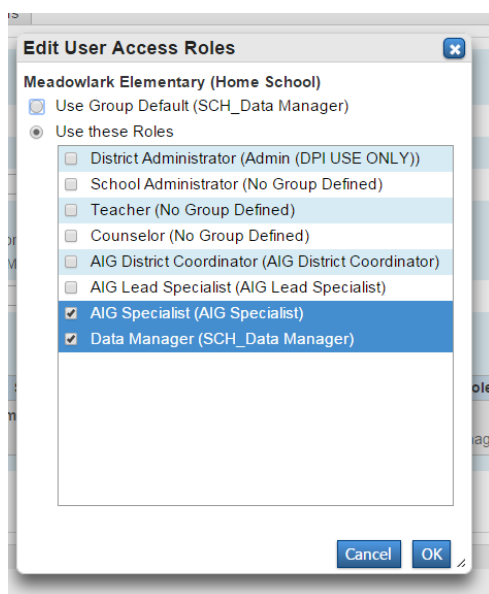
The screenshot shows the 'Roles Administration' page in PowerSchool. A role named 'AIG District Coordinator' is being created or edited. The 'Name' field is highlighted with a red box and contains 'AIG District Coordinator'. The 'Description' field is empty. The 'Enabled' checkbox is checked. The 'Group: Admin Access' section shows a dropdown menu for 'Security group assigned to the role' with 'AIG District Coordinator (148)' selected, also highlighted with a red box. At the bottom right are 'Delete' and 'Submit' buttons.

- c. Associate role with the same named group. In the **Security group assigned to this role**, select the group created in step a above.
2. AIG Lead Specialist – This person can modify records within 30 days of the record creation, change exceptionalities, and withdraw students.
  - a. Create AIG Lead Specialist security group with default "View & Modify" access, and make sure this group can see at least one student screen (e.g., Demographics). The name of the group must be exactly as stated.
  - b. Create AIG Lead Specialist role. The Description must be exactly as state: AIG Lead Specialist.
  - c. Associate role with the same named group.
3. AIG Specialist – This person has view only rights to the AIG student information.
  - a. Create AIG Specialist security group with default "View Only" access, and make sure this group can see at least one student Information screen (e.g., Demographics). The name of the group must be exactly as stated.
  - b. Create AIG Specialist role. The Description must be exactly as stated: AIG Lead Specialist.
  - c. Associate role with the same named group.
4. If additional security groups have users that will be assigned the AIG roles, these security groups need to have corresponding roles created. See below for an example:
  - a. If a current user is in a security group such as SCH-Data Manager and that user is to be the AIG District Coordinator, you must create a Data Manager role.
  - b. From Roles Administration > User Access, create a role with Description Data Manager (It doesn't have to be exactly what the security group name is but it doesn't hurt to keep them the same.)

## Setup Steps for AIG Security

- c. Associate the SCH\_Data Manager to this role.
  - d. Repeat this for any security group that you have defined that might be used to assign a user to multiple groups. Roles are used to mimic security groups to give users the ability to put one person in multiple security groups as well as the ability to assign different security permissions to a user that may wear different hats at different schools.
5. Enable Access to Page Permissions
  - a. Navigate to Start Page > System > Security > Access to Page Permissions
  - b. Turn "On" access and Submit
6. Set permissions properly on the AIG page
  - a. Navigate to Current Status AIG page for a student.
  - b. Click on "Modify access privileges for this page" at the bottom
  - c. Set all groups to access of "None" to start
  - d. Then give AIG District Coordinator and AIG Lead Specialist "Full" access privilege
  - e. Then give AIG Specialist access privilege "View Only"
  - f. Submit those changes and close the privileges mod screen by going back to step 5 and turning the access to "Off".
  - g. Repeat this process for the other two AIG tabs (Program Services and Identification Evidence).
7. To assign a user as AIG District Coordinator:
  - a. Locate the Staff user.
  - b. Click on Security Settings.
  - c. Select the Admin Access and Roles tab. The Default Group displays this user's primary security group.

**Note: This group must be defined as a role as well as a security group.**
  - d. The user has at least one school and role already defined in the Roles and Schools area.
  - e. To add an additional role, click on the pencil in the Action column to edit the record.
  - f. If the Group Default is selected, change to select Use these Roles.
    - i. Select their current role (i.e. SCH\_Data Manager).
    - ii. Select AIG District Coordinator.



- g. Click OK.



## Setup Steps for AIG Security

- h. Click Submit. The user now has the permissions of their original group plus permissions of the District coordinator.

Default Group: SCH\_Data Manager (199)




Allow Admin Sign in During These Times:

☒ Any time

☐ Allow this user's access from  to   
(Choose times between 05:00 AM and 10:00 PM)

Allowed IPs [?]:

Roles and Schools [?]

School	Roles (Group Name)	Action
Meadowlark Elementary (Home School)	AIG Specialist (AIG Specialist) Data Manager (SCH_Data Manager)	  

Add

Submit

8. To assign a user as AIG Lead Specialist:
  - a. Locate the Staff user.
  - b. Click on Security Settings.
  - c. Select the Admin Access and Roles tab. The Default Group displays this user's primary security group.

**Note: This group must be defined as a role as well as a security group.**
  - d. The user has at least one school and role already defined in the Roles and Schools area.
  - e. To add an additional role, click on the pencil in the Action column to edit the record.
  - f. If the Group Default is selected, change to select Use these Roles.
    - i. Select their current role (i.e. SCH\_Data Manager).
    - ii. Select AIG Lead Specialist.
  - g. Click OK.
  - h. Click Submit. The user now has the permissions of their original group plus permissions of the Lead Specialist.
9. To assign a user as AIG Specialist:
  - a. Locate the Staff user.
  - b. Click on Security Settings.
  - c. Select the Admin Access and Roles tab. The Default Group displays this user's primary security group.

**Note: This group must be defined as a role as well as a security group.**
  - d. The user has at least one school and role already defined in the Roles and Schools area.
  - e. To add an additional role, click on the pencil in the Action column to edit the record.
  - f. If the Group Default is selected, change to select Use these Roles.
    - i. Select their current role (i.e. SCH\_Data Manager).
    - ii. Select AIG Specialist.
  - g. Click OK.
  - h. Click Submit. The user now has the permissions of their original group plus permissions of the Specialist.
10. Additional notes:
  - a. For the District Coordinator to edit a record, once they click on Modify, the Undo button displays. They will have to delete that record and then re-add the correct information.
  - b. If the student has multiple AIG records and one of the earlier records (not the latest one) needs editing, each record from latest to earliest has to be deleted to get to the record that needs editing. It is recommended that a screen shot of the page is taken prior to editing so the user has the information needed to re-enter the records correctly.

## Setup Steps for AIG Security

---

- c. If a student still displays twice with the same information on the Headcount report, those students will still need to be submitted to support for the duplicate records to be cleaned up.
- d. If the LEA wants their users with full admin rights to be able to edit AIG records (District coordinator or Lead Specialist role), the admin group that they are in must be defined as a role. The users must be given role of Admin and role of AIG District Coordinator or AIG Lead Specialist. Just because they have full rights to PowerSchool does not give them full rights to the AIG page. **If other groups are to have read only permissions, those groups will need to be assigned the role of AIG Specialist.**

This document is the property of the NC DPI and may not be copied in whole or in part without the express written permission of the NC DPI.